CLAIMS:

1. A system (100) for processing data, the system comprising
- a first source (110) for encrypting first data, and a second source (190, 191, 199) for encrypting second data,
- a server (150) configured to obtain the encrypted first and second data, the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second sources to each other,
- computation means (110, 150, 190, 191, 199) for performing a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data.

2. The system of claim 1, wherein the second source comprises the computation means to
- obtain an encrypted inner product between the first data and the second data, and
- provide the encrypted inner product to the first source via the server,
the first source being configured to decrypt the encrypted inner product for obtaining the similarity value.

3. The system of claim 1, wherein the computation means is realized using a Paillier cryptosystem, or a threshold Paillier cryptosystem using a public key-sharing scheme.

4. The system of claim 1, wherein
the server comprises the computation means to obtain an encrypted inner product between the first data and the second data, or encrypted sums of shares of the first and second data in the similarity value, and
the server is coupled to a public-key decryption server for decrypting the encrypted inner product or the sums of shares and obtaining the similarity value.

5. The system according to any one of claims 1 to 4, wherein the similarity value is obtained using a Pearson correlation or a Kappa statistic.

6. A method of processing data, the method comprising steps of enabling to
- (210) encrypt first data for a first source, and encrypt second data for a second source,
- (220) provide the encrypted first and second data to a server that is precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second sources to each other,
- (230) perform a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data.

7. The method of claim 6, wherein the first or second data comprises a user profile of a first or second user respectively, the user profile indicating user preferences of the first or second user to media content items.

8. The method of claim 6, wherein the first or second data comprises user ratings of respective content items.

9. The method of claim 6, further comprising a step (240) of using the similarity value to obtain a recommendation of a content item for the first or second source.

10. The method of claim 9, wherein the recommendation is performed using a collaborative filtering technique.

11. A server (150) for processing data, the server being configured to
- obtain encrypted first data of a first source (110) and encrypted second data of a second source (190, 191, 199), the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second sources to each other,
- enable a computation on the encrypted first and second data to obtain a

similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data.

12. A method of processing data, the method comprising steps of

- (220) obtaining encrypted first data of a first source (110) and encrypted second data of a second source (190, 191, 199) by a server (150), the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second sources to each other,
- (230) enabling a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first sources respectively, the similarity value providing an indication of a similarity between the first and second data.

13. A computer program product enabling a programmable device when executing said computer program product to function as the system as defined in claim 1.